



Essential Elements of Information Security

Overview

This course is designed for the Information Security IS professional, and those aspiring individuals that are interested in learning more about the IS security profession. Drawing upon current standard practice methodologies and experienced experts in both federal government and private industry, this course will broaden one's general knowledge of IS security, and also address critical topics that are essential in today's security conscious environment.

In today's economic climate, keeping one's skills up-to-date could not more important. It is essential to have the skills and certifications that are necessary to go forward and to remain at the top of your field. We offer cutting-edge courses in a teaching and learning environment supplanted by an exemplary team of professional trainers that will get you where you need to be in achieving your professional career objectives.

This course is divided into the following four parts:

- Introduction to Security and Security Investigation Phase
- Security Analysis
- Logical and Physical Security Design
- Implementation and Maintenance of Security

PART I: *Introduction to Security and Security Investigation Phase*

Part 1 introduces IS security concepts by discussing:

- The history of and the need for security
- The Systems Development Life Cycle (SDLC)
- Differences between threats and attacks
- Security Ethics

Upon completion of Part I, an understanding of an organization's potential security vulnerabilities and security options will be realized.

PART II: *Security Analysis*

Part II introduces the Analysis phase of the System Development Life Cycle by outlining:

- Risk identification and assessment
- Risk management, control, and mitigation

Upon completion of Part II, an understanding of factors to consider and steps to take in analyzing a security system project will be realized.

PART III: *Logical and Physical Security Design*

Part III introduces the Design phase of the System Development Life Cycle by addressing:

- IS security policies and procedures
- IS security design models
- Incident response and disaster recovery
- Cryptography and encryption
- Physical security
- Anti-virus and SPAM

Upon completion of Part III, an understanding of standard security practices in designing a security system will be realized.

PART IV: Implementation and Maintenance of Security

Part IV introduces the Implementation and Maintenance phases of the System Development Life Cycle by summarizing:

- Project management techniques specific to IS security projects
- Implementation issues
- Organizational security functions and considerations
- Security system maintenance

Upon completion of Part IV, an understanding and recognition of industry-standard practices, processes and procedures to use when implementing and maintaining an organization's security system will be realized.

Course Requirements

Each part of this course is divided into modules. To satisfy requirements, the following must be completed:

- All course lectures
- Corresponding reading assignments
- Assessment Tests

During each lecture, class exercises will be assigned. Exercises will generally be case oriented and will be assigned individually and by group dependent upon the subject matter topic. Although these exercises will not be graded, the completion of all assignments will be valuable in applying security concepts in your current or future security professional careers.

Topical Outline

Part I

INTRODUCTION TO SECURITY AND SECURITY ANALYSIS

Modules:

- History of Security
- SDLC
- Security in the Organization
- The Need for Security
- Threats
- Attacks
- Current Issues in Information Security
- Laws & Ethics in Information Security
- How attackers use Hardware & Software to sniff traffic
- Security at the Network level
- Risk Management & Discussion Points
- Risk Assessment
- Risk Identification
- Risk Control Strategies and Mitigation Selection
- Risk Categories of Control
- Risk Assessment in Real Life
- Current Issues in Information Security Part 2, Social Engineering
- Current Deployment of Crypto Tools

Part II

SECURITY ANALYSIS

Modules:

- Risk Management & Discussion Points
- Risk Assessment
- Risk Identification
- Risk Control Strategies and Mitigation Selection
- Risk Categories of Control
- Risk Assessment in Real Life
- Current Issues in Information Security Part 2, Social Engineering
- Current Deployment of Crypto Tools

Part III

LOGICAL AND PHYSICAL SECURITY DESIGN

Modules:

- Information Security Policy, Standards, and Procedures
- System design, Security Blueprint, and Security Models
- Security Education, Training, and Awareness
- Continuity Strategy and Planning
- Incident Response, Reaction, and Recovery
- Disaster Recovery and Business Continuity
- Firewalls
- Intrusion Detection Systems
- Cryptography and Encryption Parts I & II
- Physical Security Parts I & II
- Wireless Insecurity
- Wireless Networking
- SPAM, Spyware & Viruses

Part IV

IMPLEMENTATION AND MAINTENANCE OF SECURITY

Modules:

- Project Management Phase
- Technical Topics of Implementation
- The Security Function Within an Organization's Structure
- Security Considerations Within an Organization
- Information Security Maintenance (Parts I,II,III)
- Identify Management Systems
- Security Certifications
- Course Summary & Conclusion